

April 6, 2016

**VIA FEDEX**

Computer Crime Section  
Virginia Attorney General's Office  
900 East Main Street  
Richmond, VA 23219



Kristen J. Mathews  
Member of the Firm  
d 212.969.3265  
f 212.969.2900  
kmathews@proskauer.com  
www.proskauer.com

Computer Crime Section

To Whom It May Concern:

I am writing on behalf of Proskauer Rose LLP ("Proskauer"), to inform you of an information security incident that has come to our attention. We have identified 25 Virginia residents who may have been affected.<sup>1</sup>

Proskauer received several reports from firm employees that tax returns were filed in such employees' names by unauthorized individuals in acts of identity theft. After investigating the incident, Proskauer determined that an employee in its payroll department received a fraudulent email requesting copies of W-2s of firm personnel. The email appeared to be an internal email from one of Proskauer's senior executives. Believing that the email request was legitimate, on February 28, 2016, the payroll employee emailed the requested information. The reply-to email address was fraudulent and the information was transmitted to an unauthorized third party. The information compromised consists of the information found on W-2 forms, including employee's full names and Social Security numbers.

After learning of this incident on March 31, 2016, Proskauer mailed written notification to the Virginia residents who may have been affected on April 4, 2016, and, as a precaution, Proskauer is offering these residents two years of complimentary credit monitoring services and other precautionary information and measures that they can take to safeguard their identities. Proskauer is also assisting such residents with the preparation of the forms that should be submitted to federal and state taxing authorities. Further, Proskauer has taken steps to prevent future incidents. In particular, Proskauer has enhanced staff training, improved management controls, and placed restrictions on the type of data that is electronically transmitted both within the firm, as well as outside.

For your convenience, a copy of the notice template being sent to the potentially affected residents is enclosed with this letter. If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

---

<sup>1</sup> Proskauer reserves and preserves all of its rights. Its submission of this notice does not constitute an acceptance of personal jurisdiction.

Proskauer»

April 6, 2016

Page 2

Sincerely,

*Kristen J. Mathews*  
CH

Kristen J. Mathews

**[Proskauer Letterhead with mailing address]**

April 4, 2016

**VIA FIRST CLASS MAIL**

**[address]**

Re: Notice of Data Breach

Dear [insert name]:

We are writing to tell you about a data security incident that may have exposed some of your information as an employee of the Firm. We take the protection and proper use of your information very seriously. That is why we are contacting you directly to let you know what happened, what we are doing, and what you can do.

**What Happened?**

We have received several reports from Firm employees that tax returns have been filed in their names by unauthorized individuals in acts of identity theft.

Based on our investigation, it appears that an employee in our payroll department received a fraudulent email requesting copies of W-2s of Firm personnel. The email appeared to be an internal email from one of our senior executives. Believing that the email request was legitimate, on February 28, 2016, the payroll employee emailed the requested information. The reply-to email address was fraudulent and the information was transmitted to an unauthorized third party.

We have established that the security of our information technology systems was not breached and that no other employee information, and no client information whatsoever, was compromised by this isolated incident.

**What Information Was Involved?**

The information compromised consists of the information found on W-2 forms, including your full name and Social Security number, but not that of your family members.

**What Are We Doing?**

The IRS does not hold individuals financially responsible for this type of identity theft, but if you are victimized by it, you should report it to the IRS and applicable state taxing authorities so that they can rectify the situation. We are assisting all Firm employees with the preparation of the forms that should be submitted to federal and state taxing authorities.

In addition, we are offering all employees a two-year membership in an ID theft monitoring service, ID Experts, at no cost. In order to access this service you should log on to [www.idexpertscorp.com/protect](http://www.idexpertscorp.com/protect) and use your unique code [0000000000]. You can also call them on 866-329-9984 to activate this service.

We suggest that you also actively monitor your financial account statements and the free credit reports that are available to you, and report any unauthorized activity to your bank and/or credit bureau, and to us.

Finally, we are taking steps to prevent something like this from happening again. In particular, we have enhanced staff training, improved management controls, and placed restrictions on the type of data that is electronically transmitted both within the firm, as well as outside.

### **What Can You Do?**

You can also put a "credit freeze" on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. Please note that placing a credit freeze may delay your applications for credit, mortgage, employment, housing, insurance, utilities or even cellular telephone service. The following links provide instructions for placing a credit freeze at the three national credit bureaus:

<https://www.experian.com/ncaconline/freeze>

<https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>

[https://www.freeze.equifax.com/Freeze/jsp/SFF\\_PersonalIDInfo.jsp](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)

Enclosed with this letter is additional information that may assist you to protect yourself from identity theft.

We continue to investigate this matter and will inform you of any additional information we uncover that may be helpful to you.

### **For More Information**

If you have any questions about this incident, we encourage you to contact us by telephone at 800-642-8349 (internal 13999), or by e-mail at [questions@proskauer.com](mailto:questions@proskauer.com).

We deeply regret that this incident occurred. We are committed to assisting you and taking steps to ensure that an incident like this does not happen again.

Sincerely,

Jonathan O'Brien  
*Chief Financial Officer*

## U.S. State Notification Requirements

### For residents of California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, Washington, West Virginia, and Wyoming:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with information about fraud alerts and security freezes.

#### **Equifax**

P.O. Box 740241  
Atlanta, GA 30348  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

#### **Experian**

P.O. Box 2104  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **TransUnion**

P.O. Box 6790  
Fullerton, CA 92834-6790  
1-877-322-8228  
[www.transunion.com](http://www.transunion.com)

### For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

### For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

### For residents of Illinois, Maryland and North Carolina:

State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). If you are a Maryland or North Carolina resident, you may also be able to obtain this information from your state's Attorney General.

#### **MD Attorney General's Office**

Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

#### **NC Attorney General's Office**

Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
<http://www.ncdoj.gov/>

#### **Federal Trade Commission**

Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)

### For residents of Massachusetts and West Virginia:

State laws require us to inform you of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

#### **Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

#### **TransUnion (FVAD)**

P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)